Cryptography

MATH 134 SUMMER 2022

Instructor Info

Suzana Milea

smilea@ucsc.edu

Office Hrs: TBA

Course Info

Prerequisite(s): Prerequisite(s): MATH 100 or CSE 101; MATH 110 is recommended as preparation.

Mon, Wed & Fri

09:30AM-11:50AM

Remote Instruction
(access Zoom through Canvas)

Note. Lecture recordings will be uploaded to Yuja.
The Canvas page will be updated after each class with the lecture notes and with a list of recommended homework problems.

Overview

Introduces different methods in cryptography (shift cipher, affine cipher, Vigenere cipher, Hill cipher, RSA cipher, ElGamal cipher, knapsack cipher). The necessary material from number theory and probability theory is developed in the course. Common methods to attack ciphers discussed.

Textbook

An Introduction to Mathematical Cryptography by Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman , 2nd edition, Springer, 2014.

We will cover chapters 1 to 5.

Grading Scheme

30%	Class Participation –> In class group work or quizzes
30%	Midterm Exam –> Monday Aug 15 during lecture time
40%	Take-Home Final Exam –> Due Sunday Aug 28

Grades will follow the standard scale: A: 100% to 94.0%; A-: < 94.0% to 90.0%; B+: < 90.0% to 87.0%; B: < 87.0 % to 84.0%; B-: < 84.0 % to 80.0%; C+: < 80.0 % to 77.0%; C: < 77.0 % to 74.0%; C-: < 74.0 % to 70.0%; D+: < 70.0 % to 67.0%; D: < 67.0 % to 64.0%; D-: < 64.0 % to 61.0%; F: < 61.0 % to 0.0%.

Class Communication

Ed (or 'Ed discussion') is an online threaded discussion platform that supports document and image upload, math equations, embedded video, runnable code snippets, and image annotation. Discussion board posts can be categorized, private, or even anonymous. Student responses can be 'endorsed' and instructor feedback provided. This tool is integrated in Canvas.

Course announcements will be made via Ed Discussion and NOT Canvas. Ed Discussion will be used for all communication and questions outside of lectures and office hours. Contributions to the learning of your peers will be duly noted and may result in a grade bump. If you have a question regarding homework, concepts, logistics, or anything the whole class might benefit from - post it on Ed. If your question is of a sensitive or personal nature, please send me an email. Include "MATH 134" in the subject line.

Exams

Cheating will not be tolerated. There are no make-up exams given.

In extreme circumstances, such as in the case of a medical emergency, you can make arrangements before the end of the course in order to receive an Incomplete. The notation I may be assigned, at the discretion of the faculty teaching the course, when your work for a course is of passing quality but for which some specific required work has not been completed.

Homework

The homework will be optional but highly recommended. Solutions will be provided in Canvas.

Think of the homework as your opportunity to learn the material. The goal of the homework is to gain understanding, and not just to get the right answer. If you do not understand the homework, it will be impossible to do well on the tests.

Gradescope

Assignments must be submitted via Gradescope. You don't need an extra account for Gradescope - it is integrated in Canvas. See the instructional video on how to submit an assignment. When you submit your files, you will be prompted to select, for each specified problem, the pages on which the associated work/solution are located. You are required to accurately identify the pages associated to each problem. If you fail to do so, you may lose credit for each problem for which the pages are not correctly identified. It is your responsibility to make sure your submission is legible and easy to read. If you submit work that is difficult or impossible to read, you will not receive credit for it, and you will not be allowed to resubmit.

Accommodations for Students with Disabilities

UC Santa Cruz is committed to creating an academic environment that supports its diverse student body. If you are a student with a disability who requires accommodations to achieve equal access in this course, please submit your Accommodation Authorization Letter from the Disability Resource Center (DRC) to me privately during my office hours or by appointment, preferably within the first two weeks of the quarter. At that time, I would also like us to discuss ways we can ensure your full participation in the course. I encourage all students who may benefit from learning more about DRC services to contact DRC by phone at 831-459-2089 or by email at drc@ucsc.edu.

Academic Integrity

The Mathematics Department has a zero tolerance policy towards any incident of academic dishonesty. If cheating occurs, consequences within the context of the course may range from getting zero on a particular assignment, to failing the course. In addition to these sanctions, every case of academic dishonesty is referred to the students' college Provost, who sets in motion an official disciplinary process. Cheating in any part of the course may lead to failing the course and suspension or dismissal from the university.

What is cheating? In short, it is presenting someone else's work as your own. Examples include, but are not limited to, letting someone else do your homework assignment for you, copying another student's midterm or final exam, allowing your own work to be copied, or in any way facilitating the cheating of others. Although you may discuss problems with fellow students, your collaboration must be at the level of ideas only. Legitimate collaboration ends when you "lend", "borrow", or "trade" written solutions to problems, or in any way share in the act of writing your answers.

For the full policy and disciplinary procedures on academic dishonesty, students and instructors should refer to the Academic Integrity page at the Division of Undergraduate Education: https://ue.ucsc.edu/academic-misconduct.html.

Title IX

The Title IX Office is committed to fostering a campus climate in which members of our community are protected from all forms of sex discrimination, including sexual harassment, sexual violence, and gender-based harassment and discrimination. Title IX is a neutral office committed to safety, fairness, trauma-informed practices, and due process. Title IX prohibits gender discrimination, including sexual harassment, domestic and dating violence, sexual assault, and stalking. If you have experienced sexual harassment or sexual violence, you can receive confidential support and advocacy at the Campus Advocacy Resources Education (CARE) Office by calling (831) 502-2273. In addition, Counseling Psychological Services (CAPS) can provide confidential, counseling support, (831) 459-2628. You can also report gender discrimination directly to the University's Title IX Office, (831) 459-2462. Reports to law enforcement can be made to UCPD, (831) 459-2231 ext. 1. For emergencies call 911.

Student Conduct and Community Standards

The UC Santa Cruz community includes students, staff, faculty, and others who have a vested interest in the University. As members of an academic community, integrity, accountability and mutual respect are vital pillars of being part of this community. The Principles of Community further illustrate the values and expectations set forth for being a part of this community. See https://deanofstudents.ucsc.edu/student-conduct/index.html.